CLAIMS

1. Method for configuring a firewall (1) in a computer system (2) comprising objects (3), the objects (3) for which an access control policy is established being called resources (4), characterized in that it groups the objects (3) of the system into protection domains (5, 6), each firewall (1) ensuring the protection of an internal domain (5) relative to an external domain (6), and applies to the firewall in question a rule for controlling access between a source resource (4) and a destination resource only if said source and destination resources belong to the same protection domain (5) or (6).

2. Method according to claim 1, characterized in that it determines the protection domain of the resources (4) by means of the network interfaces (10) of the firewall in question, interfaces through which the communications pass in order to reach said resources.

3. Method according to claim 2, characterized in that it defines the zones (8) comprising networks or subnetworks, in that it associates the network interfaces (10) of the firewalls to which said zones are connected with an internal or external domain, in that it determines the incoming and outgoing network interfaces (10) of the current traffic, in that it analyzes whether said network interfaces are attached to an internal or external domain, and in that it applies the rule only if both network interfaces are attached to the same internal domain (5), which corresponds to the fact that the resources belong to the same protection domain.

4. Method according to any of claims 1 through 3, characterized in that it composes groups of objects (3) for which the access control policy is identical and applies the rule between each of the resources of a source group and a destination group.

5. Method according to any of claims 1 through 4, characterized in that it characterizes the rule with a local or global scope, in that it applies the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and in that it applies the rule to all of the resources in question when the scope of the rule is global.

6. Device for implementing the method according to any of claims 1 through 5.

7. Device for configuring a firewall (1) in a computer system (2) comprising objects (3), the objects (3) for which an access control policy is established being called resources (4), characterized in that it comprises a central configuration machine (14) that makes it possible to group the objects (3) of the system into protection domains, each firewall (1) ensuring the protection of an internal domain (5) relative to an external domain (6), and to apply to the firewall in question a rule for controlling access between a source resource (4) and a destination resource only if said source and destination resources belong to the same protection domain (5) or (6).

8. Device according to claim 7, characterized in that it comprises a graphical interface (15) from which an administrator (7) can enter the protection domains (5) and (6) and the access control roles.

9. Device according to either of claims 7 and 8, characterized in that the graphical interface allows the administrator (7) to define a local or global scope for the access control rule, and in that the machine (14) applies the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applies the rule to all of the resources in question when the scope of the rule is global.

10. Software module for implementing the method according to any of claims 1 through 5.

add B2